Vincent Briganti (*pro hac vice* to be filed)
Christian P. Levis (*pro hac vice* to be filed)
Lee J. Lefkowitz (*pro hac vice* to be filed)
Matthew Acocella (*pro hac vice* to be filed)
LOWEY DANNENBERG, P.C.
44 South Broadway
White Plains, NY 10601
Tel.: (914) 997-0500
Fax: (914) 997-0035
Email: vbriganti@lowey.com
clevis@lowey.com
llefkowitz@lowey.com
macocella@lowey.com

Todd A. Seaver (SBN 271067)
Matthew D. Pearson (SBN 235339)
A. Chowning Poppler (SBN 272870)
Sarah Khorasanee McGrath (SBN 263935)
BERMAN TABACCO
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Tel.: (415) 433-3200
Fax: (415) 433-6282
Email: tseaver@bermantabacco.com
mpearson@bermantabacco.com
cpoppler@bermantabacco.com
smcgrath@bermantabacco.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

ROBERT GIRALDI, on behalf of himself and all others similarly situated;

Plaintiff,

v.

APPLE, INC., a Delaware corporation;

Defendant.

Case No.

CLASS ACTION COMPLAINT FOR DAMAGES AND EQUITABLE RELIEF

DEMAND FOR JURY TRIAL

CLASS ACTION

Plaintiff Robert Giraldi, individually and on behalf of all others similarly situated, by his undersigned counsel, alleges the following upon personal knowledge as to his own acts and upon information and belief as to all other matters.

NATURE OF THE ACTION

1. Plaintiff brings this action against defendant Apple, Inc. ("Apple" or "Defendant").

2. Apple manufactures and sells laptops, desktop computers, tablets, smartphones, and other computing devices. Part and parcel of that business is the design of central processing units ("CPUs") that power these devices. The CPUs Apple designs suffer from several defects that allow hackers to access to what was supposed to be secure data. These defects are colloquially known as Meltdown and Spectre (the "Defects").

3. The Defects cannot be "patched" (*i.e.*, fixed remotely via a software update). And any mitigation efforts would seriously affect CPU performance. Current proposals to mitigate (but not totally fix) the Defects require changes to the very root level of a computer's operating system that would degrade CPU performance by as much as 50%. So, the Defects render every chip in Apple's iPhones and iPads vulnerable. Users of the chips are left to choose: either fix the vulnerability and live with reduced CPU performance, or leave the chip vulnerable to infiltration.

4. On January 3, 2018, the news of these Defects was made public and confirmed. Two academic papers, together with blog posts and online news sources, uncovered that processors suffered from several types of design flaws and security vulnerabilities.[1]

5. Plaintiff and Class members suffered injury in fact, a loss of money/degradation in value, and damage to their property because of Apple's defective design, modification, distribution, and sale of compromised CPUs in its products.

THE PARTIES

6. Plaintiff Robert Giraldi is an individual and a citizen residing in the State of New York. In 2016, Giraldi purchased an iPhone containing an Apple A10 Fusion chip directly from

[1] *See* https://meltdownattack.com/meltdown.pdf and https://spectreattack.com/spectre.pdf

Apple at an Apple store in Williamsburg, New York. At the time of his purchase, he was not aware of the Defects. Had he known, he would not have purchased a product with this CPU or paid the price he did.

7. Apple is a business incorporated under the laws of the State of Delaware with principal place of business at 1 Infinite Loop, Cupertino, California. Apple is engaged in the business of designing, manufacturing, distributing, and selling laptops, desktop computers, tablets, smartphones, and other computing devices containing CPUs that they design, modify, and manufacture.

8. References to Apple shall mean (a) Apple's directors, officers, employees, affiliates, or agents, or anyone authorized to manage, direct, or control Apple; or (b) any persons who are the parents or alter egos of Defendant, while acting within the scope of their agency, affiliation, or employment.

JURISDICTION AND VENUE

9. The Court has general personal jurisdiction over Apple because Apple resides in this District.

10. The Court has jurisdiction under 28 U.S.C. § 1331 because at least one of Plaintiff's claims arises under the laws of the United States (*see* Count III, below, asserting a claim under the Magnuson-Moss Warranty Act, 15 U.S.C. § 2302, et. seq.).

11. The Court has jurisdiction under 28 U.S.C. § 1332(d), the Class Action Fairness Act, because the Class contains members, including Plaintiff, that are citizens of a state different from the Defendant, there are more than 100 putative Class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

12. Venue is proper in this District under 28 U.S.C. §1391(b)(2) because a substantial part of the events or omissions giving rise to these claims occurred in this District and Apple resides in this District.

INTRADISTRICT ASSIGNMENT

13. Assignment to the San Jose Division of this district is proper under Northern District of California Civil Local Rule 3-2(c) because a substantial part of the events of

omissions which give rise to the claims asserted herein occurred, and Defendant's principal place of business is located, in Santa Clara County, California. Under Civil Local Rule 3-2(e), all civil actions which arise in the county of Santa Clara shall be assigned to the San Jose Division.

FACTUAL ALLEGATIONS

14. This case concerns a security vulnerability present in, *inter alia*, processes Apple designed into its CPUs. These processes include, but are not limited to, "speculative execution" and "out-of-order execution." Apple designed and implanted these CPUs in all its iPhones, iPads, and Apple TVs, and as such every such device owned by millions are impacted by these defects.[2]

15. If a computing device like a phone or tablet were a human body, the CPU would be its brain. It controls everything and the various processes running within it. The nucleus of a CPU is the "kernel," where sensitive memory is stored (supposedly) securely. The kernel manages all processes in a device. For instance, when a user runs an application ("app") on an iPad or iPhone, the CPU dictates what processes the computer must complete. The CPU sets instructions based on what the user inputs or what the device's needs, and the CPU looks to the kernel to attain the necessary data to execute processes.

16. To execute these operations faster, a CPU predicts what it will have to do next and queues up instructions in advance. This process, called "speculative execution," allows the CPU to use what it knows about how it has operated in the past to issue a set of instructions in advance and complete them in succession. This saves times when compared to issuing instructions one at a time and executing operations in order. The CPU can even set up several conditional sets of instructions, so that one set of instructions is ready to go if it gets one input, and a different set of instructions is ready to go if it gets a different input.

17. Often, these lists of instructions will require data to execute. Sensitive data must be pulled from the CPU's kernel, a process called a "memory fetch." Ordinarily, for an app to access this sensitive data, it must satisfy certain security checks—the CPU makes sure that the app is legitimate and is supposed to be allowed to access the sensitive data. But this does not

[2] These CPUs include, but are not limited to, A4, A5, A5X, A6, A6X, A7, A8, A8X, A9, A9X, A10 Fusion and A11 Bionic processors.

happen during speculative execution. So, when a CPU queues up instructions in advance, it conducts memory fetches to have the necessary data at the ready (stored in a "cache") for when the instructions are going to be executed. This is the failing at the heart of the Defects.

18. In reporting on this scourge of Defects in these chips, the New York Times analogized speculative execution to a butler bringing glasses of wine to a user:

> In a way, modern microprocessors act like attentive butlers, pouring that second glass of wine before you knew you were going to ask for it.
>
> But what if you weren't going to ask for that wine? What if you were going to switch to port? No problem: The butler just dumps the mistaken glass and gets the port. Yes, some time has been wasted. But in the long run, as long as the overall amount of time gained by anticipating your needs exceeds the time lost, all is well.
>
> Except all is not well. Imagine that you don't want others to know about the details of the wine cellar. It turns out that by watching your butler's movements, other people can infer a lot about the cellar. Information is revealed that would not have been had the butler patiently waited for each of your commands, rather than anticipating them. Almost all modern microprocessors make these butler movements, with their revealing traces, and hackers can take advantage.[3]

A. Background

19. A CPU is supposed to keep each app on an iPhone, iPad, or Apple TV—and the data the apps rely on—isolated from one another. This principle, called "memory isolation," is an important concept in systems design. Without memory isolation, malware could capture data stored in apps, or stored in a computer's memory. For instance, a user's credit card information, bank information, passwords, e-mails, etc., which might be stored in a browser or an e-mail app, must be kept within the access of that app only.

20. The Defects, known as Meltdown and Spectre, are vulnerabilities in Apple's devices' CPUs, caused by how Apple designed, modified, and manufactured those CPUs to access memory.

[3] *The Looming Digital Meltdown*, The New York Times, *available at* https://www.nytimes.com/2018/01/06/opinion/looming-digital-meltdown.html?action=click&module=Well&pgtype=Homepage (Last accessed Jan. 8, 2018)

B. CPUs

21. Typically, a CPU will isolate the memory pages (where data are stored) of the kernel from everything else. Access is controlled by a "supervisor bit," which, like an air traffic controller, signals whether a given program is allowed to access a particular memory page in the kernel. This "supervisor bit" can only be set when entering kernel code, and it gets cleared when switching to another user process. So, where one program might get authorization to execute a memory fetch and attain data from the kernel, another program running at the same time might be blocked. Executing a memory fetch, however, takes time because it requires the CPU to stop executing regular instructions and switch from "user mode" into a special "kernel mode," before entering the kernel to access memory. The CPU must then switch back to user mode after it leaves the kernel to resume executing regular instructions.

22. To save time, an Apple CPU only checks whether a program is allowed to access data from a memory fetch *after* speculative execution—or another, similar process, "out-of-order execution"[4]—occurs. Speculative execution sets up branches of possible future processes and increases performance by guessing these likely future processes in each branch. And true to its name, speculative execution even prematurely executes these possible future instructions. Thus, Apple CPUs can freely access kernel memory when performing speculative or out-of-order execution.

23. When a process in a speculative execution branch depends on certain uncached data located in memory, as discussed above, it takes time to fetch. Rather than wasting time idling and waiting for the fetch to complete, the processor speculatively sets up the program on various guessed paths. When the data eventually arrives from memory, the processor checks if its guess was correct. If wrong, the processor discards the (incorrect) speculative executions and reverts, resulting in performance comparable to if the CPU had simply waited for the fetch. To

[4] Out-of-order execution is where CPUs queue up instructions for the running of a program in a "reorder buffer," and then "retire" them in the correct execution order. This is done to save time: it allows a program's instructions to be executed in parallel with, and sometimes before, instructions that would normally precede—as opposed to executing processes one after the other. At times, this path of the execution of instructions branches off. In other words, one set of instructions is contingent upon a preceding instruction going a certain way.

use the New York Times' analogy, above: this is the butler discarding the incorrect glass of wine he preemptively poured and instead going to fetch the correct glass of port.

24. But if the guess was correct, the CPU commits to the correctly-guessed process and yields a time-saving performance gain because work was done during what would normally be idle time.

25. To improve speculative execution, Apple designed, modified, and manufactured its CPUs to map recently executed branch instructions to help guess future ones. So, to increase the accuracy of these speculative guesses, processors use a Branch Target Buffer ("BTB") to predict future code addresses based on past executions.

26. These queued up conditional branches of fetched memory should be blocked. But we now know it is possible for attackers to read the data by exploiting the Defects.

C. Meltdown

27. Meltdown allows an attacker to run code to access a dump of an entire kernel address space, including its memory.

28. Meltdown can do this because speculative execution memory fetches are stored in the cache. Many of these speculative memory fetches do not get used. Ordinarily, these cache-stored memory fetches are discarded if they do not ultimately get authorized and utilized by a process. The CPU cache is not supposed to be readable if the memory is correctly isolated. But by using a cache "timing attack," a rogue process can determine whether data are held in the cache, even if it does not have authority to read those data.

29. A timing attack is a type of "side-channel" attack, which means it is based on side-effects of normal computer operations that inadvertently leak information. Common examples of side-channel attacks are hackers analyzing sound leaks, electromagnetic leaks, or amounts of power consumed by a computer. This allows a hacker to glean what the computer was doing, based on what would have made that precise sound, leaked precisely that amount of electromagnetism, or consumed precisely that much power. A "timing attack" does this based on analyzing the passage of time. An attacker monitors how much time certain functions took to execute and then reverse engineers *what the computer did* based on *how long it took to do it*.

30. Here, an attacker can use timing to discern whether secret data have been cached. For example, if an instruction to read the data uses the cache to do so, it happens fast. If the data are not cached, the CPU would have to request that the data be read from memory (which is slower). The attacker can use this difference in timing to detect which of these took place, and whether the data was already in the cache or not.

31. From that, the attacker can discern the location of the data on the memory and read every memory address by repeating these steps for any and all memory locations, effectively resulting in a dump of the entire kernel memory.

D. Spectre

32. Spectre allows malicious software to run code that will induce a system to perform operations that would not normally occur, but which leak data. And unlike Meltdown, Spectre is not a single type of vulnerability, but rather a class of multiple potential vulnerabilities.

33. Because BTB can touch private data even before a process is deemed to have authority to access the data, the attacker can use speculative execution to reach otherwise secret memory. The attacker searches for places where speculation touches upon otherwise inaccessible data. The attacker exploits the processor's BTB activity by manipulating how it guesses future executions of a conditional branch.

34. Spectre does this by performing operations designed to incorrectly train a processor to later make an exploitable speculative prediction, turning the CPU's own processes of speculative execution against it. Then, the processor speculatively executes these mis-instructions. Thus, the attacker tricks the processor to use speculative execution to access secret data and store it in the cache, resulting in a transfer of data from the memory to the cache.

35. Then, the attacker times the side effect of the processor being faster (as a result of the fact that its mistrained machinery is bound to load a cache line). In this way, an attacker can force speculative execution to read any data from the memory at any address and store the memory in the cache. Then, knowing the data is in the cache, the attacker modifies the cache state to expose the data and recovers it.

E. Apple

36. Starting in 2010, with the release of the iPhone 4 and the original iPad, all Apple mobile devices have contained custom ARM-based CPUs designed by Apple. ARM Holdings, a British designer of CPUs, develops and patents CPU architecture and then licenses it other companies, including Apple. Apple takes it from there, adding its own design touches to the licensed architecture and making the processors its own. As such, while many companies could use ARM-based chips in their products, they are all different. Some companies might use ARM-based chips without modification, others customize the chips. The ARM-based chips in Apple's devices are uniquely Apple, and the chips are used exclusively in Apple products: specifically iPhones, iPads, and Apple TVs made since 2010, when Apple started customizing the chips.

37. Therefore, ARM-based chips are not automatically impacted by Spectre and Meltdown, but many are. Apple's chips are impacted by Spectre and Meltdown because Apple chooses to turn on speculative execution and out-of-order execution to improve speed. We now know that improvement to speed comes at the cost of security.

38. Apple's chips utilize out-of-order execution and speculative execution, subjecting Apple devices to Meltdown and Spectre, and making the devices vulnerable to infiltration. More important, the devices' exposure to Meltdown and Spectre means that the devices are, in some cases, not patchable or, in other cases, would be significantly slowed where patching is possible.

39. Apple is aware that its devices suffer from the Defects and admits that "Security researchers have recently uncovered security issues known by two names, Meltdown and Spectre. These issues apply to all modern processors and affect nearly all computing devices and operating systems. All Mac systems and iOS devices are affected . . . ."[5]

F. Mitigation Is Impracticable or Impossible

40. The Defects are material because neither Plaintiff, Class members, nor any reasonable consumer would have purchased Apple devices, or paid the prices they did, had they known data stored on their systems would be compromised.

[5] *See* https://support.apple.com/en-us/HT208394

41. The Defects are unprecedented in scope in that they expose millions of Apple devices to the vulnerabilities because Apple designed its processors to use speculative execution and out-of-order execution in this unprotected way. To date, any proposed patches to cure these security vulnerabilities will result in substantial performance degradation.

42. Any steps to mitigate the Defects would require extensive changes at the root levels of the operating system software, which would impact the performance of Apple's processor-based machines. For example, experts have proposed moving the kernel to a separate address space, but switching between two address spaces for every memory fetch takes time, resulting in a computer running slower. In another example, experts have proposed adding speculative execution blocking instructions. In other words, a conditional branch speculative execution can be halted if a path is particularly sensitive. Again, the problem is that doing so would severely degrade performance.

43. And this highlights the difference between Spectre and Meltdown. Meltdown exploits scenarios where CPUs allow out-of-order execution of *user* instructions to read kernel memory. Thus, the above mitigation proposals (which would result in degraded performance, anyway) that prevent speculative execution of instructions in certain user processes from accessing kernel memory, would not do anything to mitigate Spectre. Spectre exploits scenarios where CPUs speculatively execute instructions that can be read from memory that a process could access on its own. Simply put: Spectre can manipulate a CPU into revealing its own data. On the other hand, Meltdown can be used to read privileged memory in a process's address space that even the process itself would normally be unable to access (on some unprotected operating systems, this includes data belonging to the kernel or other processes).

G. Apple's Knowledge of the Security Vulnerabilities

44. Apple knew of the Defects long ago. ARM Holdings PLC, the company that licenses the architecture to Apple (which Apple modifies) with which Apple designs its chips, admits that it was notified of the Security Vulnerabilities in June 2017 by Google's Project Zero and that it immediately notified its architecture licensees who build on and modify the architecture and create their own processor designs (like Apple). Various news outlets have

reported that "Apple, Linux, and Microsoft have known about the issue for several months."[6] In fact, the researchers who discovered the Defects note in their academic paper that: "Using the practice of responsible disclosure, we have disclosed a preliminary version of our results to Intel, AMD, ARM, Qualcomm as well as to other CPU vendors. We have also contacted other companies including Amazon, Apple, Microsoft, Google and others."[7] Nonetheless, Apple continued and continues to sell these products containing the Defects.

CLASS ACTION ALLEGATIONS

45. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of himself and as representative of the following Class:[8]

> All persons who purchased or leased one or more iPhones, iPads, or Apple TVs from Apple and/or its authorized retailer sellers or products containing CPUs designed by Apple, at any time since January 1, 2010.

46. Excluded from the Class are Defendant, its officers and directors, management, employees, subsidiaries, or affiliates. Also excluded from the Class is the Judge presiding over this action, his or her law clerks, spouse, any other person within the third degree of relationship living in the Judge's household, the spouse of such person, and the United States Government.

47. The Class is so numerous that joinder of the individual members of the proposed Class is impracticable. The Class includes thousands of persons geographically dispersed throughout the United States. The precise number and identities of Class members are unknown to Plaintiff, but are known to Defendant or can be ascertained through discovery, using records of sales, warranty records, and other information kept by Defendant or its agents.

48. Plaintiff does not anticipate any difficulties in the management of this action as a class action. The Class is ascertainable, and there is a well-defined community of interest in the questions of law and/or fact alleged herein since the rights of each Class member were

[6] https://www.macrumors.com/2018/01/04/apple-meltdown-spectre-vulnerability-fixes/

[7] https://spectreattack.com/spectre.pdf, at 3.

[8] Plaintiff has defined the Class based on currently available information and hereby reserves the right to amend the definition of the Class, including, without limitation, membership criteria and the Class Period.

infringed or violated in similar fashion based upon Defendant's uniform misconduct. Notice can be provided through sales and warranty records and publication.

49. Plaintiff's claims are typical of the claims of the other members of the Class. Plaintiff and the members of the Class sustained damages arising out of Defendant's common course of conduct in violation of law as complained of herein. The injuries and damages of each member of the Class were directly caused by Defendant's wrongful conduct in violation of the laws as alleged herein.

50. Plaintiff will fairly and adequately protect the interests of the members of the Class. Plaintiff is an adequate representative of the Class and has no interest that is adverse to the interests of absent Class members. Plaintiff has retained counsel competent and experienced in class action litigation.

51. Questions of law or fact common to the Class exist as to Plaintiff and all Class members, and these common questions predominate over any questions affecting only individual members of the Class. Among these predominant common questions of law and/or fact are the following:

a) Whether Defendant's CPUs possess Defects and the nature of the Defects;

b) Whether Defendant made any implied warranties in connection with the sale of the defective CPUs;

c) Whether Defendant breached any implied warranties relating to its sale of defective CPUs by failing to resolve the Defects in the manner required by law;

d) Whether Defendant was unjustly enriched by selling defective Apple devices;

e) Whether Defendant violated applicable consumer protection laws by selling CPUs with the Defects or by failing to disclose the Defects, and failing to provide the relief required by law; and

f) The appropriate nature and measure of Class-wide relief.

52. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff and the Class. Individual questions, if any, pale by comparison to the numerous common questions that predominate.

53. A class action is superior to other available methods for the fair and efficient group-wide adjudication of this controversy, and individual joinder of all Class members is impracticable, if not impossible, because a large number of Class members are located throughout the United States. Moreover, the cost to the court system of such individualized litigation would be substantial. Individualized litigation would likewise present the potential for inconsistent or contradictory judgments and would result in significant delay and expense to all parties and multiple courts hearing virtually identical lawsuits. By contrast, the conduct of this action as a class action presents fewer management difficulties, conserves the resources of the parties and the courts, protects the rights of each Class member and maximizes recovery to them.

54. Defendant has acted on grounds generally applicable to the entire Class, thereby making final injunctive relief or corresponding declaratory relief appropriate with respect to the Class as a whole.

COUNT I
Breach of Implied Warranty

55. Plaintiff hereby incorporates all the above allegations by reference as if fully set forth herein. Plaintiff asserts this count individually and on behalf of the proposed Class.

56. Defendant and its authorized agents and resellers sold Apple devices to Plaintiff and Class members in the regular course of business.

57. Defendant impliedly warranted to members of the general public, including Plaintiff and Class members, that these CPUs were of merchantable quality (*i.e.*, a product of a high enough quality to make it fit for sale, usable for the purpose it is made, of average worth in the marketplace, or not broken, unworkable, damaged, contaminated, or flawed), was of the same quality as those generally acceptable in the trade or that would pass without objection in the trade, were free from material defects, and were reasonably fit for the ordinary purposes for which they were intended or used. In addition, Defendant either was or should have been aware of the particular purposes for which such CPUs are used, and that Plaintiff and the

Class members were relying on the skill and judgment of Defendant to furnish suitable goods for such purpose.

58. Plaintiff and the Class purchased their Apple devices either directly from Defendant or through Defendant's authorized agents and re-sellers. Pursuant to agreements between Defendant and its authorized agents and re-sellers, the stores from which Plaintiff and/or Class members purchased their defective Apple devices are authorized retailers and authorized CPU service facilities. Plaintiff and Class members are third-party beneficiaries of, and substantially benefited from, such contracts.

59. Defendant breached its implied warranties by selling Plaintiff and Class members defective Apple devices. The Defects render the CPUs in Apple devices, and therefore the devices themselves, unmerchantable and unfit for their ordinary or particular use or purpose. Defendant has refused to recall, repair, or replace, free of charge, all Apple devices or any of their defective component parts or refund the prices paid for such CPUs.

60. The Defects in the Apple devices' CPUs existed when the devices left Defendant's and its authorized agents' and retail sellers' possession and thus are inherent in such CPUs and devices.

61. As a direct and proximate result of Defendant's breach of its implied warranties, Plaintiff and Class members have suffered damages and continue to suffer damages, including economic damages at the point of sale in terms of the difference between the value of the CPUs as warranted and the value of the CPUs as delivered. Additionally, Plaintiff and Class members either have or will incur economic, incidental, and consequential damages in the cost of repair or replacement and costs of complying with continued contractual obligations as well as the cost of buying an additional CPU they would not have purchased had the CPUs in question not contained the non-repairable Defects.

62. Plaintiff and Class members are entitled to legal and equitable relief against Defendant, including damages, specific performance, rescission, attorneys' fees, costs of suit, and other relief as appropriate.

COUNT II
Breach of Express Warranty

63. Plaintiff hereby incorporates all the above allegations by reference as if fully set forth herein. Plaintiff asserts this count individually and on behalf of the proposed Class.

64. Defendant warranted that Apple devices were free of Defects when it sold the devices to Plaintiff and members of the Class as described herein. Under the terms of Apple's warranty, each covered Apple device came with an express warranty that warrants that the device will be free from defects in materials and workmanship under normal use during the warranty period.

65. Defendant also marketed the increase in speed and performance in its CPUs. After implementation of security patches against the Defects, the speed and performance of Defendant's CPUs are not as represented.

66. Plaintiff and the Class purchased their Apple devices either directly from Defendant or through Defendant's authorized agents and re-sellers. Plaintiff and the Class relied on Defendant's express warranty when purchasing their Apple devices. Pursuant to agreements between Defendant and its authorized agents and re-sellers, the stores from which Plaintiff and/or Class members purchased their defective Apple devices (for Class members who did not purchase their defective devices directly from Defendant) are authorized retailers and authorized CPU service facilities. Plaintiff and Class members are third-party beneficiaries of, and substantially benefited from, such contracts.

67. As a direct and proximate result of Apple's breach of warranty, Plaintiff and each of the Class members have suffered damages and continue to suffer damages.

68. As a direct and proximate result of Defendant's breach of warranty, Plaintiff and Class members have suffered damages and continue to suffer damages, including economic damages at the point of sale in terms of the difference between the value of the CPUs as warranted and the value of the CPUs as delivered. Additionally, Plaintiff and Class members either have or will incur economic, incidental, and consequential damages in the cost of repair or replacement and costs of complying with continued contractual obligations as well as the

cost of buying an additional CPU they would not have purchased had the CPUs in question not contained the non-repairable Defects.

69. Plaintiff and Class members are entitled to legal and equitable relief against Defendant, including damages, specific performance, rescission, attorneys' fees, costs of suit, and other relief as appropriate.

COUNT III
The Magnuson-Moss Warranty Act, 15 U.S.C. § 2302, et seq.

70. Plaintiff incorporates all of the above allegations by reference as if fully set forth herein.

71. Plaintiff asserts this claim individually and on behalf of all Class members.

72. Plaintiff satisfies the Magnuson-Moss Warranty Act ("MMWA") jurisdictional requirement because he alleges diversity jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2).

73. Plaintiff and Class members are "consumers" within the meaning of the MMWA, 15 U.S.C. § 2301(4)-(5).

74. Apple is a "supplier" and "warrantor" within the meaning of 15 U.S.C. sections 2301(4)-(5).

75. Apple devices are "consumer products" within the meaning of 15 U.S.C. § 2301(1).

76. The MMWA provides a cause of action for any consumer who is damaged by the failure of a warrantor to comply with a written or implied warranty. 15 U.S.C. § 2310(d)(1).

77. Defendant expressly and impliedly warranted to members of the public, including Plaintiff and Class members, that these CPUs were free of defects and otherwise merchantable and fit for the ordinary and particular purposes for which the CPUs are required and used.

78. Defendant has breached its express and implied warranties because the Apple devices sold to Plaintiff and Class members were not as warranted and were otherwise not merchantable nor fit for the ordinary and particular purposes for which such goods are used in

that the CPUs suffer from a critical security defect, requiring an operating system-level remedial measure that will degrade the performance of the CPU.

79. Plaintiff and the Class purchased their Apple devices either directly from Defendant or through Defendant's authorized agents and re-sellers. Pursuant to agreements between Defendant and its authorized agents and re-sellers, the stores from which Plaintiff and/or Class members purchased their defective Apple devices are authorized retailers and authorized CPU service facilities. Plaintiff and Class members are third-party beneficiaries of, and substantially benefited from, such contracts.

80. As a direct and proximate result of Defendant's breach of its express and implied warranties, Plaintiff and the Class Members sustained damages and other losses in an amount to be determined at trial. Apple's conduct damaged Plaintiff and the Class, who are entitled to recover damages, specific performance, diminution in value, costs, attorneys' fees, rescission, and/or other relief as may be appropriate.

COUNT IV
Violations of New York General Business Law § 349

81. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint as though stated herein.

82. Plaintiff Giraldi and the other members of the Class have been injured and suffered damages by violations of section 349(a) of New York General Business Law (the "GBL"), which states that deceptive acts or practices in the conduct of any business, trade, or commerce or in the furnishing of any service in the State of New York are unlawful.

83. Defendant engaged in acts and practices in the State of New York that were deceptive or misleading in a material way, and that injured Plaintiff Giraldi and other members of the Class.

84. Specifically, Defendant engaged in deceptive acts or practices by selling CPUs knowing or being aware the CPUs contained a critical security defect. Defendant also engaged in unfair business acts or practices by making warranties, which it refuses to honor. As a direct and

proximate result of these violations, Plaintiff and the Class suffered actual damages as discussed herein.

85. Plaintiff and Class members used Defendant's products and had business dealings with Defendant either directly or indirectly as described above. The acts and practices of Defendant have caused Plaintiff and Class members to lose money and property by being overcharged for and paying for the defective CPUs at issue, or being required to purchase an additional non-defective CPU. Plaintiff Giraldi and members of the Class have been damaged by Defendant's violations of Section 349 of the GBL, for which they seek recovery of the actual damages they suffered because of Defendant's willful and wrongful violations of section 349, in an amount to be determined at trial.

COUNT V
Violations of New York General Business Law § 350

86. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

87. New York GBL § 350 prohibits false advertising in the conduct of any business, trade, or commerce.

88. New York GBL § 350 defines false advertising as "advertising, including labeling, of a commodity . . . if such advertising is misleading in a material respect."

89. Defendant's advertisements were false and misleading in a material way due to false labeling, statements, and omissions regarding the performance and security of its products.

COUNT VI
Unjust Enrichment

90. Plaintiff incorporates all of the above allegations by reference as if fully set forth herein. Plaintiff asserts this claim individually and on behalf of all Class members.

91. This cause of action is alleged as an alternative to the warranty claims as permitted under Rule 8(d)(2) of the Federal Rules of Civil Procedure.

92. As Plaintiff and the Class show just grounds for recovering money paid for benefits Defendant received from them, either directly or indirectly, and they have a right to

restitution at law through an action derived from the common-law writ of assumpsit by implying a contract at law based on principles of restitution and unjust enrichment, or though quasi-contract.

93. Defendant, having received such benefits, is required to make restitution. The circumstances here are such that, as between the two, it is unjust for Defendant to retain such benefit based on the conduct described above. Such money or property belongs in good conscience to the Plaintiff and Class members and can be traced to funds or property in Defendant's possession. Plaintiff and Class members have unjustly enriched Defendant through payments and the resulting profits enjoyed by Defendant as a direct result of such payments. Plaintiff's detriment and Defendant's enrichment were related to and flowed from the conduct challenged in this Complaint.

94. By virtue of the purchase and sale of the CPUs in question, Defendant alternatively entered into a series of implied-at-law or quasi-contracts that resulted in money being had and received by Defendant, either directly or indirectly, at the expense of Plaintiff and Class members under agreements in assumpsit. Plaintiff and other Class members conferred a benefit upon Defendant by purchasing one of the defective CPUs. Defendant had knowledge of the general receipt of such benefits, which Defendant received, accepted, and retained. Defendant owes Plaintiff and Class members these sums that can be obtained either directly from Class members, Defendant, or its authorized retailers.

95. Under principles of restitution, an entity that has been unjustly enriched at the expense of another by the retention of benefit wrongfully obtained is required to make restitution to the other. In addition, under common law principles recognized in claims of common counts, assumpsit, unjust enrichment, restitution, and quasi-contract, under the circumstances alleged herein it would be inequitable for Defendant to retain such benefits without paying restitution or restitutionary damages. Such principles require Defendant to return such benefits when the retention of such benefits would unjustly enrich Defendant. They should not be permitted to retain the benefits conferred by Plaintiff and Class members via

payments for the defective CPUs. Other remedies and claims may not permit them to obtain such relief, leaving them without an adequate remedy at law.

96. Plaintiff and Class members seek appropriate monetary relief for such claims. Based on the facts and circumstances alleged above, in order to prevent unjust enrichment and to prevent Defendant from taking advantage of its own wrongdoing, Plaintiff and the Class are further entitled to the establishment of a constructive trust, in a sum certain, of all monies charged and collected or retained by Defendant from which Plaintiff and Class members may seek restitution.

COUNT VII
Strict Liability

97. Plaintiff incorporates all of the above allegations by reference as if fully set forth herein. Plaintiff asserts this claim individually and on behalf of all Class members.

98. Plaintiff and the Class were harmed by CPUs Defendant manufactured, which were contained in, but also separate and apart from, the devices they purchased.

99. Defendant's CPUs contained a manufacturing defect, or were defectively designed for the reasons set forth above.

100. Plaintiff and Class members have been harmed, as they now own a device with a CPU that due to such manufacturing or design defect is subject to invasion of a supposedly core protected part of the CPU and decreased performance, in an amount according to proof at trial.

COUNT VIII
Negligence

101. Plaintiff incorporates all of the above allegations by reference as if fully set forth herein. Plaintiff asserts this claim individually and on behalf of all Class members.

102. Defendant was negligent in the manufacture and design of the CPUs containing the Defects, which CPUs were contained in, but also separate and apart from, the devices that Plaintiff and Class members purchased.

103. Defendant's negligence was a substantial factor and reasonably foreseeable in causing harm to Plaintiff and Class members.

104. Plaintiff and Class members have been harmed, as they now own a device with a CPU that due to such manufacturing or design defect is subject to invasion of a supposedly core protected part of the CPU and decreased performance, in an amount according to proof at trial.

PRAYER FOR RELIEF

Plaintiff demands relief as follows:

A. That the Court certify this lawsuit as a class action under Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, that Plaintiff be designated as class representative, and that Plaintiff's counsel be appointed as counsel for the Class;

B. That Defendant be permanently enjoined and restrained from continuing and maintaining the violation alleged in the Complaint;

C. Awarding Plaintiff and Class members all proper measures of monetary relief and damages, plus interest to which they are entitled;

D. Awarding equitable, injunctive, and declaratory relief as the Court may deem just and proper, including restitution and restitutionary disgorgement;

E. That the Court award Plaintiff and the Class their costs of suit, including reasonable attorneys' fees and expenses, as provided by law; and

F. That the Court direct such further relief as it may deem just and proper.

///

///

///

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff demands a jury trial as to all issues triable by a jury.

DATED: January 11, 2018

BERMAN TABACCO

By: */s/ Todd A. Seaver*
Todd A. Seaver

Matthew D. Pearson
A. Chowning Poppler
Sarah Khorasanee McGrath
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Tel.: (415) 433-3200
Fax: (415) 433-6282
Email: tseaver@bermantabacco.com
mpearson@bermantabacco.com
cpoppler@bermantabacco.com
smcgrath@bermantabacco.com

Vincent Briganti (*pro hac vice* to be filed)
Christian P. Levis (*pro hac vice* to be filed)
Lee J. Lefkowitz (*pro hac vice* to be filed)
Matt Acocella (*pro hac vice* to be filed)
LOWEY DANNENBERG, P.C.
44 South Broadway
White Plains, NY 10601
Tel.: (914) 997-0500
Fax: (914) 997-0035
Email: vbriganti@lowey.com
clevis@lowey.com
llefkowitz@lowey.com
macocella@lowey.com

Attorneys for Plaintiff